Plano Analítico: Segurança de Informação em Redes e Sistemas

1. Identificação da Unidade Curricular

- **Curso:** Engenharia de Redes e Telecomunicações (ERT)
- **Ano:** 5º | **Semestre:** 1º
- **Créditos:** 8.0 UC
- **Carga Horária Total:** 120 Horas
- **Distribuição:**
    - **Teóricas (T):** 30h
    - **Teórico-Práticas (TP):** 30h
    - **Práticas/Laboratório (P):** 30h
    - **Trabalho Autónomo (TA):** 22h
    - **Orientação e Tutoria (OT):** 4h
    - **Avaliação (AV):** 4h

---

1. Fundamentação

Num mundo hiperconectado, a segurança não é um acessório, mas uma fundação. Esta disciplina fundamenta-se na necessidade de mitigar riscos, detetar intrusões e responder a incidentes. Para o engenheiro de ERT, é vital dominar tanto a segurança de perímetro (Firewalls, IPS) como a segurança de dados (Criptografia) e de sistemas (Hardening), garantindo a continuidade dos serviços face a ameaças persistentes.

2. Objectivos Instrutivos e Educativos

- **Instrutivos:** Compreender os princípios de segurança e gestão de risco; dominar algoritmos de criptografia simétrica e assimétrica; configurar infraestruturas de chaves públicas (PKI); implementar firewalls, VPNs e sistemas de deteção de intrusão (IDS); estudar a segurança em camadas (Defesa em Profundidade).
- **Educativos:** Fomentar a ética profissional e a responsabilidade legal (*Ethical Hacking*); desenvolver o rigor na aplicação de políticas de segurança e promover a cultura de proteção de dados e privacidade.

3. Resultado de Aprendizagem

O estudante será capaz de:

- Analisar vulnerabilidades em redes e sistemas utilizando ferramentas de auditoria.
- Projetar arquiteturas de rede seguras com zonas desmilitarizadas (DMZ).
- Implementar protocolos de comunicação seguros (IPsec, TLS/SSL, SSH).

- Configurar políticas de controlo de acesso e autenticação multifator (MFA).
- Responder a incidentes de segurança seguindo protocolos internacionais.

4. Planeamento Temático (8 UC)

Tema	Horas (T+TP+P)	Conteúdo Programático
I. Introdução e Gestão de Risco	15h	A Tríade CID; Ameaças, Ataques e Vulnerabilidades; Normas ISO/IEC 27001 e 27002.
II. Criptografia e Autenticação	25h	Criptografia Clássica e Moderna (AES, RSA, ECC); Funções Hash; Assinaturas Digitais e Certificados (X.509).
III. Segurança de Perímetro	30h	Firewalls (Stateful, Next-Gen); DMZ; IDS/IPS; VPNs (IPsec e SSL/TLS); Segurança em Redes Sem Fios (WPA3).
IV. Segurança de Sistemas e Aplicações	25h	Hardening de SO; Segurança em Web e E-mail; Proteção contra Malware; Segurança em Cloud e Contentores.
V. Auditoria e Resposta a Incidentes	25h	Análise de vulnerabilidades (Nmap, Nessus); Testes de penetração básicos; Forense digital básica; Planos de Continuidade.

---

5. Recomendações Metodológicas

- **Laboratório de Cibersegurança (30h):** Uso de ambientes isolados (**Kali Linux**) para testes de penetração éticos e ferramentas de defesa como **pfSense** ou **Cisco ASA**.
- **CTF (Capture The Flag):** Realização de competições práticas para resolver desafios de criptografia e invasão controlada.
- **Análise de Malware:** Estudo de casos reais de ataques (ex: Ransomware) e como as redes poderiam ter sido protegidas.

6. Sistema de Avaliação

Conforme a alocação de **4h para AV**:

- **Avaliação Contínua (60%):** Projeto de auditoria e segurança de uma rede empresarial (40%) e relatórios de laboratórios de criptografia/firewall (20%).
- **Avaliação Formal (40%):** Exame escrito focado nos fundamentos teóricos e mecanismos de defesa.

7. Bibliografia Principal Indicada

1. **STALLINGS, William.** *Criptografia e Segurança de Redes*. Pearson.
2. **FOROUZAN, Behrouz A.** *Cryptography and Network Security*. McGraw-Hill.

3. **KIM, David & SOLOMON, Michael.** *Fundamentals of Information Systems Security*. Jones & Bartlett Learning.